DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Operazioni Sospette e reati informatici: lo "spettro" degli Iban Virtuali

23 Giugno2026

Fabio Cristini, Compliance, Risk & AML Manager, Kiron Partner S.p.A.

Fabio Cristini, Compliance, Risk & AML Manager, Kiron Partner S.p.A.

Con la Comunicazione dell'8 giugno scorso, l'UIF ha delineato le principali modalità con cui i *reati informatici* possono contribuire a realizzare *operazioni sospette* che si concretizzano in fenomeni di riciclaggio attraverso l'utilizzo della tecnologia, con la conseguenza di rendere maggiormente difficoltosa la tracciabilità della provenienza dei fondi, successivamente reimmessi sul mercato dei capitali tramite il ricollocamento in attività profittevoli e il reinvestimento degli stessi (c.d. schema classico: *placement*, *layering*, *integration*).

Proprio nella fase della stratificazione, valenza cardine assume l'utilizzo di articolati strumenti finanziari e di pagamento che consentono al denaro proveniente da reato di rientrare nella sfera lecita degli investimenti tramite circolarizzazioni di somme, giustificate con causali ideate *ad hoc* per il conseguente *trasferimento continuativo e frazionato di fondi* tra diversi conti di pagamento intestati a *soggetti terzi*, la cui identità si rivela complessa da individuare sia quanto all'ordinante sia quanto all'effettivo beneficiario dell'operazione.

Tra gli strumenti utilizzati per la circolarizzazione organizzata delle transazioni finanziarie, ruolo centrale assume il c.d. *Iban Virtuale*.

La definizione di "IBAN", *alias* International Bank Account Number, è rilevabile nel Regolamento (UE) n. 260/2012 (SEPA), quale «*numero identificativo di conto bancario di pagamento internazionale che individua, senza ambiguità, un unico conto di pagamento in uno Stato membro*».

A fronte di tale ambito tradizionale, il virtual IBAN è, invece, qualificato nel nuovo Regolamento (UE) n. 1624/2024 c.d. Anti-Money Laundering Regulation (AMLR) come "*un identificativo che fa sì che i pagamenti siano reindirizzati verso un conto di pagamento identificato da un IBAN diverso da tale identificativo*".

A seconda dei casi, il virtual IBAN può essere emesso a nome dell'utente finale o a favore di un altro intermediario, il quale attribuisce poi il vIBAN all'utente finale.

Il servizio viene solitamente qualificato come *accessorio* rispetto ad un *Master Account*: i codici vIBAN mutuano dall'IBAN principale la sigla del Paese e il codice della banca, distinguendosi però dai codici dell'IBAN principale per: a) *l'identificativo della filiale*, non corrispondente nei codici vIBAN ad un'unità

vedi l'articolo online

organizzativa fisica; b) il *numero di conto, che può contenere caratteri distintivi, funzionali a rendere subito individuabile la natura virtuale dell'IBAN* o anche a consentire al cliente di personalizzare una parte del codice.

Risulta, inoltre, utile distinguere tra IBAN virtuali utilizzati come conti secondari del Master Account, utili ad esempio alle imprese per riconciliare i flussi finanziari e categorizzare i pagamenti al fine di associarli a diversi fornitori ricorrenti e i vIBAN utilizzati, invece, come *veri e propri conti separati rispetto al Master Account*.

In quest'ultimo caso, i vIBAN sono offerti da un prestatore di servizi di pagamento (PSP) a un altro PSP, che, a sua volta, li mette a disposizione dei propri clienti per consentire loro di ricevere o disporre bonifici anche a favore di terzi ovvero permettere la generazione di vIBAN con differenti codici Paese, da associare ad un unico Master Account[1].

In tale ultima ipotesi vengono a configurarsi, da un lato, (i) un rapporto di conto tra il prestatore del Master Account e il titolare del medesimo e, dall'altro, (ii) altri separati rapporti di conto tra il titolare del Master Account stesso e gli utilizzatori finali dell'IBAN virtuale.

Pur avendo tale secondo meccanismo la finalità "nobile" di superare la c.d. discriminazione da IBAN[2], emergono tuttavia *possibili rilevanti anomalie* collegate all'utilizzo dei Virtual IBAN per scopi di *riciclaggio e finanziamento del terrorismo*.

La UIF ha sottolineato come, in alcuni casi, conti apparentemente registrati in Europa siano in realtà vIBAN forniti da Prestatori di Servizi di Pagamento (PSP) con sede in paesi extra-UE, potenzialmente impiegati per attività di riciclaggio di denaro di provenienza sospetta.

1 Si veda quanto diffusamente e compiutamente descritto da FC Hub nell'articolo https://fchub.it/iban-virtuali-prime-indicazioni-da-parte-di-banca-ditalia-e-delluif/.

2 Con "*discriminazione da IBAN*" si fa riferimento al caso in cui una persona non possa inviare o ricevere un bonifico SEPA dal/sul proprio conto bancario, poiché lo stesso risulta situato in uno Stato diverso rispetto a quello del beneficiario/ordinante. Resta fermo però che l'art. 9 del Regolamento SEPA (UE n. 260/2012) vieta qualsiasi limitazione basata sull'origine geografica del conto all'interno dell'UE.

A questo proposito, il regolamento (UE) 1624/2024, all'art. 22, par. 3, stabilisce anzitutto che l'ente prestatore/emittente vIBAN è tenuto a mettere a disposizione del fornitore del *Master Account*, senza indugio su richiesta specifica, le informazioni che identificano e verificano l'identità effettiva della persona fisica che utilizza il vIBAN.

Come autorevolissima dottrina cita[3], una regolamentazione è certamente necessaria al fine di garantire che le autorità di vigilanza chiariscano che i soggetti obbligati all'AML non debbano generare confusione tra i clienti, in ossequio anche alla disciplina generale della trasparenza.

Sul piano transfrontaliero, poi, l'IBAN virtuale può altresì generare concreti rischi di aggiramento della supervisione bancaria. Esso, infatti, ben si presta a mascherare la nazionalità del reale prestatore del servizio, sicché potrebbe accadere che i prestatori di servizi di pagamento extracomunitari utilizzino tale schema per accedere al mercato senza autorizzazione.

Posto quanto sopra, di massima utilità al fine di evidenziare i rischi del Virtual Iban sul piano AML si rivela la Comunicazione congiunta Banca Italia-UIF ormai consolidata sull'argomento.

Nel documento, vengono anzitutto delineati gli scenari a maggior rischio di riciclaggio:

- coinvolgimento di terze parti ("OBO"): di regola, è prevista la verifica autonoma del soggetto terzo rispetto alla ricorrenza di *bad* e *sanctions lists*, ma risulta opportuno effettuare altresì l'acquisizione di informazioni ulteriori (es. paese di insediamento e fatturato e settore di attività economica) utili per attribuire un punteggio di rischio AML al soggetto assegnatario del vIBAN e, se del caso, per aggiornare quello del cliente intestatario del conto di pagamento;

- uso di vIBAN da parte di clienti a loro volta soggetti obbligati ai sensi del d. lgs. 231/2007. Sono stati osservati casi di utilizzo di vIBAN da parte di operatori in valute virtuali (CASP) o PSP, ad esempio IP o IMEL, che li assegnano ai propri clienti per riconciliare più agevolmente gli scambi di flussi con ciascuno di essi. Questo caso rileva, su un piano generale, sotto il profilo della collaborazione nello scambio di informazioni tra soggetti obbligati. Ad esempio, sarebbe opportuno

3 Raffaele Lener, *Regolazione Fintech e Testo Unico Bancario*, Quaderni di Ricerca Giuridica Banca Italia, 2024.

vedi l'articolo online

prevedere *presidi contrattuali in forza dei quali il PSP/CASP si vincola a collaborare con la banca sul fronte antiriciclaggio* e a *fornire opportune informazioni*, ad esempio, sull'adeguata verifica condotta sui propri clienti in relazione ai quali, come nei casi sopra descritti, gestisce pagamenti tramite vIBAN e ad agevolare lo scambio informativo a fini di collaborazione attiva.

Alla luce di quanto sopra, le primarie indicazioni di Vigilanza in merito a tali fenomeni a maggior rischio sono individuabili nelle seguenti prassi conformative:

- porre in essere, nei confronti degli assegnatari di vIBAN, tutti gli adempimenti previsti per *l'identificazione e la verifica del titolare effettivo*. In particolare, ai sensi delle Disposizioni della Banca d'Italia in materia di adeguata verifica, al momento dell'instaurazione del rapporto o all'atto dell'assegnazione dei vIBAN, se successivo, gli intermediari dovranno identificare e verificare l'identità dell'assegnatario del vIBAN (sia esso una persona fisica o un soggetto diverso da una persona fisica) e del suo eventuale titolare effettivo adottando, con riferimento a quest'ultimo caso, misure proporzionate al rischio per ricostruirne, con ragionevole attendibilità, l'assetto proprietario e di controllo. Il cliente si dovrà inoltre impegnare a fornire tempestivamente, nel corso del rapporto, le informazioni necessarie per l'identificazione di ogni nuovo assegnatario di vIBAN che intenda associare al master account;

- in sede di apertura del rapporto, *definire quale sia lo specifico utilizzo (scopo) che il cliente intende fare dei vIBAN* e *ricostruire, in particolare, eventuali finalità di tipo OBO*. I vIBAN sono solitamente richiesti da clientela con complesse esigenze di riconciliazione. Gli intermediari dovrebbero, pertanto, porre particolare attenzione a ricostruire *lo scopo e la natura del rapporto* nei casi in cui la richiesta di vIBAN provenga da clientela che non abbia tali esigenze. In tale specifico caso, occorrerà porre particolare attenzione alla circostanza che il *titolare del master account sia legittimato, sulla base di un'apposita delega*, a ricevere, detenere e movimentare i fondi dei terzi assegnatari dei vIBAN, per conto dei quali agisce.

  Nell'attività di controllo costante del rapporto, i PSP che offrano vIBAN sono tenuti a monitorare l'operatività del cliente per assicurare la *coerenza tra la finalità inizialmente dichiarata e il concreto utilizzo che viene fatto del master account cui sono associati i vIBAN*. A tal fine, risulta particolarmente utile analizzare separatamente l'operatività riconducibile a ciascun vIBAN, in quanto la mera analisi dell'operatività complessiva del master account potrebbe rivelarsi insufficiente sia a intercettare eventuali *modalità di utilizzo dei vIBAN per conto terzi*, non dichiarate dal cliente, sia a evidenziare operatività anomale riferite ai singoli assegnatari di vIBAN, nel caso di operatività di tipo "OBO";

- buone prassi sono infine la *raccolta, in sede di adeguata verifica, di informazioni sui presidi antiriciclaggio adottati dal cliente titolare del master account* che farà uso dei vIBAN e l'introduzione di *presidi contrattuali in forza dei quali* il titolare del master account si vincola a collaborare concretamente con il PSP di radicamento di tale master account sul fronte antiriciclaggio e a fornire informazioni, ad esempio, sull'adeguata verifica condotta sui clienti in relazione ai quali gestisce pagamenti tramite vIBAN o ad agevolare lo scambio informativo.

Infine, allo scopo di mitigare gli impatti sulla capacità del sistema di individuare vIBAN e di ricostruire correttamente i flussi finanziari, le Autorità richiamano la buona prassi di inserire, nelle cifre finali dell'IBAN dedicate al numero di conto, *caratteri distintivi funzionali a rendere subito individuabile la natura virtuale dell'IBAN* (ad esempio, le *lettere VA o V all'inizio del campo relativo al numero di conto*). Dell'eventuale presenza di tali caratteri distintivi dovranno tenere conto tutti i soggetti obbligati nelle attività di monitoraggio transazionale della propria clientela.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it